AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method, comprising the computer-implemented steps of:

receiving trust information defining one or more trusted signatories;

receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;

receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and two or more digital signatures of the hostname and the one or more configuration directives;

wherein the configuration information includes the particular configuration directive;

wherein the two or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, and a second digital signature of a second portion of the one or more configuration directives by a second user;

attempting to verify the two or more digital signatures based on the trust information and the security information;

verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the one or more configuration directives on the host network element;

wherein, in accordance with the collective authority, the first user is responsible for the first portion of the one or more configuration directives, the second user is responsible for the second portion of the one or more configuration directives, and the first portion and the second portion of the one or more configuration directives are to be applied to the host network element at the same time;

applying the one or more configuration directives to the host network element only when the two or more digital signatures are verified successfully;

wherein applying the one or more configuration directives comprises applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals;

wherein the steps of the method are performed by the host network element.

2-3. (Canceled)

4. (Previously Presented) A method as recited in Claim 1, wherein applying the particular configuration directive comprises applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures.

5. (Previously Presented) A method as recited in Claim 1, wherein the two or more digital signatures use public key cryptography, and wherein public keys for the two or more digital signatures are stored on the host.

6. (Previously Presented) A method as recited in Claim 1, wherein the two or more digital signatures use public key cryptography, wherein public keys for the two or more digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the two or more digital signatures.

7. (Previously Presented) A method as recited in Claim 1, wherein the two or more digital signatures use public key cryptography, and wherein public keys for the two or more digital signatures are received in a digital certificate and extracted from the digital certificate as part of attempting to validate the two or more digital signatures.

8. (Previously Presented) A method, comprising the computer-implemented steps of:
receiving trust information defining one or more trusted signatories;
receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives;
receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, one or more

digital signatures of the hostname and configuration directives, and a date-time value;

determining if the date-time value is within the time period;

determining if the one or more configuration directives have been previously received during the time period; and

only when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period, attempting to verify the one or more digital signatures based on the trust information, and applying the configuration directives to the host network element only when the one or more digital signatures are verified successfully;

wherein the steps of the method are performed by the host network element.

9. (Original) A method as recited in Claim 8, wherein the step of determining if the one or more configuration directives have been previously received during the time period comprises the steps of:

generating a secure hash of the one or more configuration directives;

determining if the secure hash is found in memory.

10. (Original) A method as recited in Claim 8, wherein the step of determining if the one or more configuration directives have been previously received during the time period comprises the steps of:

generating a secure hash of the one or more configuration directives;

determining if the secure hash is found in non-volatile memory.

11. (Original) A method as recited in Claim 8, further comprising the step of storing the secure hash in non-volatile memory, in association with an expiration value, when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period.

12. (Previously Presented) A method as recited in Claim 8, further comprising the steps of:

verifying that the one or more digital signatures is valid and that one or more principals respectively associated with the digital signatures have collective authority to perform the directives on the host network element.

13. (Original) A method as recited in Claim 8, further comprising the steps of:
receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;
applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals.

14. (Original) A method as recited in Claim 8, further comprising the steps of:
receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;
applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures.

15. (Original) A method as recited in Claim 8, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures are stored on the host.

16. (Original) A method as recited in Claim 8, wherein the digital signatures use public key cryptography, wherein public keys for the digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the digital signatures.

17. (Original) A method as recited in Claim 8, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures received in a digital certificate and extracted from the digital certificate as part of attempting to validate the digital signatures.

18. (Previously Presented) A method for verifying configuration changes for network devices using digital signatures, comprising the computer-implemented steps of:

receiving a public key for a user of the network devices;

receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives to a specified network device;

receiving configuration information comprising a hostname, one or more configuration directives for the specified network device associated with the hostname, one or more digital signatures of the hostname and configuration directives, and a date-time value;

determining if the date-time value is within the time period;

determining if the one or more configuration directives have been previously received during the time period, by generating a secure hash of the one or more configuration directives and determining if the secure hash is found in memory; and

only when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period, performing the steps of:

attempting to verify the one or more digital signatures based on generating a secure hash of the one or more configuration directives using the public key and comparing the secure hash to the one or more digital signatures, and applying the configuration directives to the specified network device only when the one or more digital signatures are verified successfully;

wherein the steps of the method are performed by the specified network device.

19. (Currently Amended) A method as recited in any of Claims ~~1,~~ 8[[,]] or 18, wherein the one or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature.

20. (Previously Presented) A method as recited in any of Claims 8 or 18, wherein the one or more digital signatures comprise a first digital signature of a first portion of the

one or more configuration directives by a first user, a second digital signature of a second portion of the one or more configuration directives by a second user, and a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature.

21. (Currently Amended) A computer-readable volatile or non-volatile medium storing one or more sequences of instructions for verifying configuration changes for network devices using digital signatures, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving trust information defining one or more trusted signatories;

receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;

receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and two or more digital signatures of the hostname and the one or more configuration directives;

wherein the configuration information includes the particular configuration directive;

wherein the two or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, and a second digital signature of a second portion of the one or more configuration directives by a second user;

attempting to verify the two or more digital signatures based on the trust information and the security information;

verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the one or more configuration directives on the host network element;

wherein, in accordance with the collective authority, the first user is responsible for the first portion of the one or more configuration directives, the second user is responsible for the second portion of the one or more configuration directives, and the first portion and the second portion of the one or more configuration directives are to be applied to the host network element at the same time;

applying the one or more configuration directives to the host network element only when the two or more digital signatures are verified successfully;

wherein applying the one or more configuration directives comprises applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals.

22. (Canceled)

23. (Currently Amended) A computer-readable volatile or non-volatile medium as recited in Claim 21, ~~wherein the two or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user,~~ wherein the second digital signature is applied to a resultant of the first digital signature.

24. (Previously Presented) A computer-readable volatile or non-volatile medium as recited in Claim 21, wherein the two or more digital signatures further comprise a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature.

25. (Currently Amended) An apparatus for verifying configuration changes for network devices using digital signatures, comprising:

means for receiving trust information defining one or more trusted signatories;

means for receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;

means for receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and two or more digital signatures of the hostname and the one or more configuration directives;

wherein the configuration information includes the particular configuration directive;

wherein the two or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, and a second

digital signature of a second portion of the one or more configuration directives by a second user;

means for attempting to verify the two or more digital signatures based on the trust information and the security information;

means for verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the one or more configuration directives on the host network element;

wherein, in accordance with the collective authority, the first user is responsible for the first portion of the one or more configuration directives, the second user is responsible for the second portion of the one or more configuration directives, and the first portion and the second portion of the one or more configuration directives are to be applied to the host network element at the same time;

means for applying the one or more configuration directives to the host network element only when the two or more digital signatures are verified successfully;

wherein the means for applying the one or more configuration directives comprise means for applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals.

26. (Canceled)

27. (Currently Amended) An apparatus as recited in Claim 25, ~~wherein the two or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user,~~ wherein the second digital signature is applied to a resultant of the first digital signature.

28. (Previously Presented) An apparatus as recited in Claim 25, wherein the two or more digital signatures further comprise a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature.

29. (Currently Amended) An apparatus for verifying configuration changes for network devices using digital signatures, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving trust information defining one or more trusted signatories;

receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;

receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and two or more digital signatures of the hostname and the one or more configuration directives;

wherein the configuration information includes the particular configuration directive;

wherein the two or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, and a second digital signature of a second portion of the one or more configuration directives by a second user;

attempting to verify the two or more digital signatures based on the trust information and the security information;

verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the host network element;

wherein, in accordance with the collective authority, the first user is responsible for the first portion of the one or more configuration directives, the second user is responsible for the second portion of the one or more configuration directives, and the first portion and the second portion of the one or more

configuration directives are to be applied to the host network element at the same time;

applying the one or more configuration directives to the host network element only when the two or more digital signatures are verified successfully;

wherein applying the one or more configuration directives comprises applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals.

30. (Canceled)

31. (Currently Amended) An apparatus as recited in Claim 29, ~~wherein the two or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user,~~ wherein the second digital signature is applied to a resultant of the first digital signature.

32. (Previously Presented) An apparatus as recited in Claim 29, wherein the two or more digital signatures further comprise a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature.

33. (Canceled)

34. (Previously Presented) A computer-readable volatile or non-volatile medium as recited in Claim 21, wherein the instructions that cause the one or more processors to perform the step of applying the particular configuration directive comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures.

35. (Previously Presented) A computer-readable volatile or non-volatile medium as recited in Claim 21, wherein the two or more digital signatures use public key cryptography, and wherein public keys for the two or more digital signatures are stored on the host network element.

36. (Previously Presented) A computer-readable volatile or non-volatile medium as recited in Claim 21, wherein the two or more digital signatures use public key cryptography, wherein public keys for the digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the two or more digital signatures.

37. (Previously Presented) A computer-readable volatile or non-volatile medium as recited in Claim 21, wherein the two or more digital signatures use public key cryptography, and wherein public keys for the two or more digital signatures are received in a digital certificate and extracted from the digital certificate as part of attempting to validate the two or more digital signatures.

38. (Canceled)

39. (Previously Presented) An apparatus as recited in Claim 25, wherein the means for applying the particular configuration directive comprise means for applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures.

40. (Previously Presented) An apparatus as recited in Claim 25, wherein the two or more digital signatures use public key cryptography, and wherein public keys for the two or more digital signatures are stored on the host network element.

41. (Previously Presented) An apparatus as recited in Claim 25, wherein the two or more digital signatures use public key cryptography, wherein public keys for the two or

more digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the two or more digital signatures.

42. (Previously Presented) An apparatus as recited in Claim 25, wherein the two or more digital signatures use public key cryptography, and wherein public keys for the two or more digital signatures are received in a digital certificate and extracted from the digital certificate as part of attempting to validate the two or more digital signatures.

43. (Canceled)

44. (Previously Presented) An apparatus as recited in Claim 29, wherein the instructions that cause the processor to perform the step of applying the particular configuration directive comprise instructions which, when executed by the one or more processors, cause the processor to perform the step of applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures.

45. (Previously Presented) An apparatus as recited in Claim 29, wherein the two or more digital signatures use public key cryptography, and wherein public keys for the two or more digital signatures are stored on the host network element.

46. (Previously Presented) An apparatus as recited in Claim 29, wherein the two or more digital signatures use public key cryptography, wherein public keys for the two or more digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the two or more digital signatures.

47. (Previously Presented) An apparatus as recited in Claim 29, wherein the two or more digital signatures use public key cryptography, and wherein public keys for the two or more digital signatures are received in a digital certificate and extracted from the digital certificate as part of attempting to validate the two or more digital signatures.

48. (New) A computer-readable volatile or non-volatile medium storing one or more sequences of instructions which, when executed by one or more processors, cause the one or more processors to perform steps comprising:

receiving trust information defining one or more trusted signatories;

receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives;

receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, one or more digital signatures of the hostname and configuration directives, and a date-time value;

determining if the date-time value is within the time period;

determining if the one or more configuration directives have been previously received during the time period; and

only when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period, attempting to verify the one or more digital signatures based on the trust information, and applying the configuration directives to the host network element only when the one or more digital signatures are verified successfully.

49. (New) The computer-readable volatile or non-volatile medium as recited in Claim 48, wherein the instructions that cause determining if the one or more configuration directives have been previously received during the time period comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

generating a secure hash of the one or more configuration directives;

determining if the secure hash is found in memory.

50. (New) The computer-readable volatile or non-volatile medium as recited in Claim 48, wherein the instructions that cause determining if the one or more configuration directives have been previously received during the time period comprise instructions

which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

generating a secure hash of the one or more configuration directives;

determining if the secure hash is found in non-volatile memory.

51. (New) The computer-readable volatile or non-volatile medium as recited in Claim 48, wherein the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of storing the secure hash in non-volatile memory, in association with an expiration value, when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period.

52. (New) The computer-readable volatile or non-volatile medium as recited in Claim 48, wherein the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of:

verifying that the one or more digital signatures are valid and that one or more principals respectively associated with the digital signatures have collective authority to perform the directives on the host network element.

53. (New) The computer-readable volatile or non-volatile medium as recited in Claim 48, wherein the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;

applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals.

54. (New) The computer-readable volatile or non-volatile medium as recited in Claim 48, wherein the one or more sequences of instructions further comprise instructions which,

when executed by the one or more processors, cause the one or more processors to perform the steps of:

receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;

applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures.

55. (New) The computer-readable volatile or non-volatile medium as recited in Claim 48, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures are stored on the host network element.

56. (New) The computer-readable volatile or non-volatile medium as recited in Claim 48, wherein the digital signatures use public key cryptography, wherein public keys for the digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the digital signatures.

57. (New) The computer-readable volatile or non-volatile medium as recited in Claim 48, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures are received in a digital certificate and extracted from the digital certificate as part of attempting to validate the digital signatures.

58. (New) The computer-readable volatile or non-volatile medium as recited in Claim 48, wherein the one or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature.

59. (New) The computer-readable volatile or non-volatile medium as recited in Claim 48, wherein the one or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, a second digital

signature of a second portion of the one or more configuration directives by a second user, and a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature.

60. (New) A computer-readable volatile or non-volatile medium storing one or more sequences of instructions for verifying configuration changes for network devices using digital signatures, which instructions, when executed by one or more processors, cause the one or more processors to perform steps comprising:

receiving a public key for a user of the network devices;

receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives to a specified network device;

receiving configuration information comprising a hostname, one or more configuration directives for the specified network device associated with the hostname, one or more digital signatures of the hostname and configuration directives, and a date-time value;

determining if the date-time value is within the time period;

determining if the one or more configuration directives have been previously received during the time period, by generating a secure hash of the one or more configuration directives and determining if the secure hash is found in memory; and

only when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period, performing the steps of:

attempting to verify the one or more digital signatures based on generating a secure hash of the one or more configuration directives using the public key and comparing the secure hash to the one or more digital signatures, and

applying the configuration directives to the specified network device only when the one or more digital signatures are verified successfully.

61. (New) The computer-readable volatile or non-volatile medium as recited in Claim 60, wherein the one or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature.

62. (New) The computer-readable volatile or non-volatile medium as recited in Claim 60, wherein the one or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, a second digital signature of a second portion of the one or more configuration directives by a second user, and a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature.